Identification of safety risks in mixed traffic concepts in industrial sites

Tiusanen R.[1]., Berger J.[1] & Malm T.[1]

[1] VTT Technical Research Centre of Finland Ltd

KEYWORDS: autonomous, work machine, conceptual design, hazard identification, risk assessment

ABSTRACT

Automated driving technologies are developing rapidly for off-road vehicles and industrial machinery. However, highly automated heavy industrial vehicles and work machines still need to be separated from manual machines and human workforce. Different operating environments and work processes require different solutions to ensure efficient and safe operation and interaction with autonomous or semi-autonomous machines. The traditional system safety analysis methods like Preliminary Hazard Analysis (PHA) and Operating Hazard Analysis (OHA) have been successfully applied in different domains and different automated machinery applications. These methods continue to have an important meaning when they are effectively used in the system safety engineering. However, these methods do not cover or consider autonomy aspects especially safety critical interactions and their possible deviations between system controllers (human and technical). The new challenge is that machine's autonomous behaviour cannot be fully predetermined because the key element in machine autonomy is adaptability to dynamically changing environment based on the perception of the available information. There is need for new methods to be able to identify and analyse autonomy related uncertainties, hazards, and hazardous situations. The System-Theoretic Process Analysis method (STPA) brings in new views for the analysis of autonomy aspects by supporting the identification and analysis of unsafe control actions in different hierarchy levels of the system control. STPA method includes the modelling of the hierarchical control structure of the machinery system and complements the perspectives of traditional system safety methods. STPA method provides a formal presentation to connect losses, system level hazards, possible unsafe control actions and loss scenarios so that this information can be used for defining system safety requirements. This study is part of the EU and Business Finland funded research project 'Artificial Intelligence using Quantum measured Information for real-time distributed systems at the edge' (A-IQ Ready). The safety research in the project aims for improving safety and productivity of automated vehicle operations outdoors in co-existence with human workers in so called 'mixed traffic' operations. The main target of the safety research is to develop data fusion concepts and risk conscious situational awareness information for autonomous driving and load handling.

1 INTRODUCTION

According to the general systems engineering approach, risk management decisions in the system-development process are made systematically as the system development proceeds [1]. In practice, the design decisions to reduce safety risks are based on comparison of alternative solutions at different layers of protection and prediction. The systematic and clearly phased safety engineering approach and risk assessment process supports the development of machine autonomy when selecting operating concepts and technological solutions. New methods and tools are needed when designing interactions between autonomous machines and human operators in safety critical decision-making situations. Advanced safety engineering procedures need to be in place to not only identify and control new safety risks, but also to document and communicate safety-related aspects between all relevant stakeholders [2]. In industrial logistic systems an interesting and challenging vision is to enable autonomous machines, manual machines, and manual workers to operate and collaborate in the same operating area. This is called a 'mixed traffic' or 'mixed mode' operation. For 'mixed traffic' operation concepts, it is crucial to develop new principles and criteria for converting situational awareness information and site information into a dynamic "risk awareness" component, which can then be integrated into the situational awareness system of automated operation.

In the A-IQ Ready project there are two different industrial case systems utilising an autonomous vehicle for transportation. Both systems are operating in a semi-restricted industrial area where there is other traffic using the same roadways. In this paper we focus on the autonomous transportation system developed for saw log transportation in a sawmill environment. The other system includes automated container handling operations and autonomous container transportation in an intermodal terminal environment.

In the case system, the saw logs are transported using a very low diesel-powered autonomous vehicle. The vehicle carries the saw logs in a 'cage' specially built for this purpose. The vehicle lifts and lowers the cage in loading and unloading places. The material handling machine drivers in the loading and unloading points operate the autonomous transportation process by commanding the vehicle to to pick-up or drop down the cage and to move between certain cage places at the site. Figure 1 illustrates the situation where the autonomous vehicle drives under the full saw log cage. Two examples of possible traffic situations on the route of the autonomous vehicle are illustrated in Figure 2. The green vehicles in the figure represent manually driven vehicles.

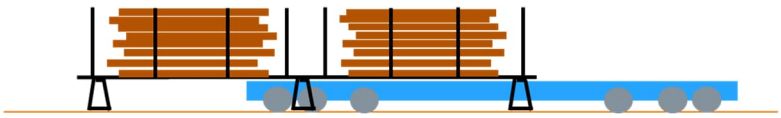

Figure 1 An outline of the situation where the autonomous vehicle drives under the full saw log cage

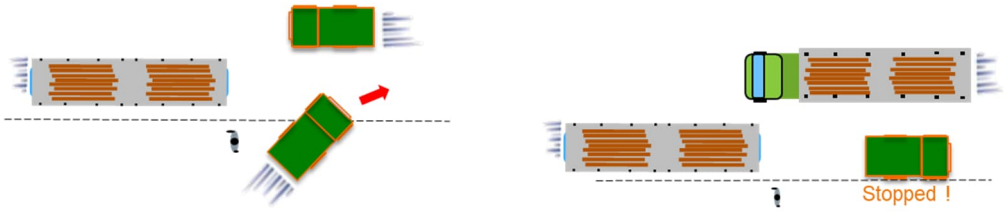

Figure 2 Two examples of possible traffic situations in the route of the autonomous vehicle

The purpose of this study was to study how System Theoretic Process Analysis (STPA) method could support identification of safety risks and potential problems related to autonomous operation and especially autonomous driving at industrial sites in early conceptual design phase of the logistic system. The approach for hazard identification and risk assessment in this study was a combination of Preliminary Hazard Analysis (PHA) method and STPA method. This paper briefly describes the case system under study, introduces the analysis methods and presents and discusses the main findings of the study.

2 RISK ANALYSIS APPROACH

In this study the approach for hazard identification and risk assessment was a combination of PHA method and STPA method used in early conceptual phase of the system design process.

2.1 Preliminary hazard analysis (PHA)

The analysis of the autonomous saw log transportation concept was first conducted by using the PHA method. PHA is a semi-quantitative analysis that is performed to identify all potential hazards and accidental events that may lead to an accident, to rank the identified accidental events according to their severity, and to identify required safety measures and follow-up actions. The typical steps in PHA are: PHA prerequisites; hazard identification; course and consequence estimation; and risk ranking and follow-up actions. PHA is described more in detail e.g., by Rausand (2005) [3].

Estimation of the negative safety consequences for humans and the magnitude of the material damage or production losses to vehicles or infrastructure was done by using the following categories. Severity of safety consequences were assessed with three categories: death of a person or several persons; permanent injury; reportable injury. Material damages or production losses were assessed with two categories: material damage to the autonomous vehicle, to other vehicles or to the infrastructure; interruption of the logistic work process or other transportation processes and traffic.

Estimation of the probability of hazardous situations in daily operation was done by using three categories: rare; possible; probable in daily operations. Assessment of the magnitude of the risks (risk = probability x severity) was done by using three categories: High risk = Unacceptable risk. Changes must be done before the use of the system.

Medium risk = Undesirable risk. Changes must be made to minimize the risk. Low risk = Tolerable risk. Changes must be made to minimize the risk if it is possible.

2.2 System theoretic process analysis (STPA)

Systems-Theoretic Process Analysis (STPA) is a relatively recent hazard analysis method based on Systems-Theoretic Accident Model and Processes (STAMP). STAMP is an accident causality model based on systems theory, considering safety as a control problem instead of focusing on failures or human errors. The STPA process has been described in STPA Handbook [4]. So far there is no application specific STPA guideline or standard for mobile machinery industry, but in 2022 SAE has published a guideline of STPA method for the evaluation of safety-critical systems in automotive industry: SAE J3187:2022 'System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems'[5]. STPA method consists of four main phases or steps as follows (Figure 3)[4]:

- Step 1 defines the scope and limitations of the analysis, losses, hazards, and safety constraints.
- In Step 2, the system is modelled as a hierarchical control structure, which is a system model composed of feedback control loops. This is a graphical representation featuring controllers and controlled processes represented as rectangles, and the interactions between them (control and feedback) represented as arrows. The hierarchy is illustrated by the vertical axis, i.e., the highest control authority is at the top of the diagram.
- In Step 3, the control structure is systematically analysed to find unsafe control actions (UCAs) that, in a particular context and worst-case situations, can lead to a hazard.
- Step 4 concludes the analysis with the identification of loss scenarios, which describe the causal factors that can lead to UCAs and hazards.

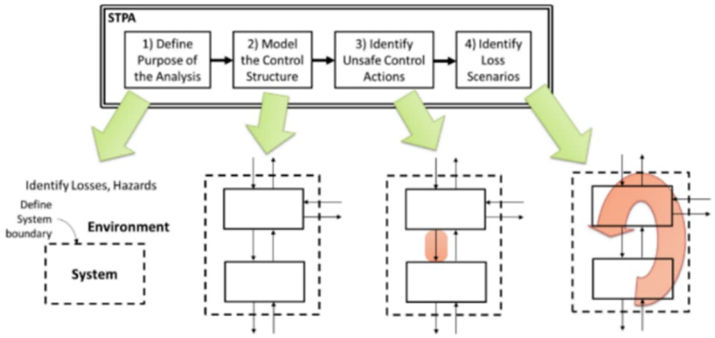

Figure 3 Four steps of STPA method [4]

STPA describes the system as a hierarchical control structure consisting of feedback loops, intending to incorporate various causal factors, including software aspects, as well as human and organizational factors. STPA provides a systematic procedure to identify flaws within the safety of the system control structure [3]. The STPA handbook also provides a checklist to support the identification of case specific loss scenarios based on the two main types of loss scenarios. The two general loss scenario types can be identified by asking the following questions [4]:

- Why would a control action become unsafe, leading to hazards?
- Why would a control action be improperly executed or not executed, leading to hazards?

3 RESULTS

The aim of PHA was to identify the most important hazards and hazardous situations, related to the autonomous transportation in mixed traffic context, to analyse their causes and consequences and to assess the significance of the safety risks caused by them. In the PHA, hazards and dangerous situations were identified and analysed at a general level. In early conceptual design phase, there were not yet more information about operating procedures, traffic situations at the site or detailed information of control system functionalities.

The main autonomy related safety hazards in this case were overrunning or crushing a person or collision with a vehicle on the roadway. If the autonomous vehicle does not recognize an obstacle in front and runs over a pedestrian or cyclist, the consequences are fatal. If a person is crushed between unexpectedly moving vehicle and

cage structures, a person dies or is permanently injured. If the autonomous vehicle collides with another vehicle, it can cause injury to the vehicle driver and passengers and both vehicles are damaged. A falling log on a person from the full cage due to an unexpected stop or faulty loading of the saw logs can also have fatal consequences. As a result of the PHA, a set of clear system-level safety requirements and important aspects to be considered in the safety planning of the mixed traffic operating concept were revealed. Some examples of the technical requirements are shown below.

- The safety system of the autonomous vehicle must be capable of detecting an obstacle, a pedestrian, a cyclist, or a vehicle in its path and near its path from such a distance that it is able to stop and prevent an accident under all circumstances.
- Unexpected start-up or movements (or driving direction) of the autonomous vehicle must be prevented.
- The operators in the loading or unloading points must be able to stop the autonomous vehicle remotely.
- Failure in the safety system of the autonomous vehicle, its driving control system or in the wireless communication system must stop the vehicle and prevent the vehicle from moving.

When analysing the hazardous situations, it was clearly noted that safe operation in mixed fleet context requires the commitment of everyone operating in the area to the new concept and compliance with safety instructions and traffic rules. Not all dangerous situations can be prevented or foreseen with the help of technical solutions alone. Some examples of the traffic rules and safety instructions to enable safe mixed traffic operation are shown below.

- Safety instructions for material handling in loading and unloading points.
- Traffic rules and safety instructions for pedestrians and cyclists in the area.
- Traffic rules, safety instructions and parking instructions in the area.
- Vehicle drivers must follow the traffic rules and safety instructions.
- Traffic rules for intersections when the autonomous vehicle is approaching the intersection area.
- Persons working or visiting the area must follow the rules and instructions.

The starting point for STPA in the first step was the system descriptions and the PHA results which were turned to definitions for losses, system level hazards, and system level safety constraints. In the second step together with the company representatives of the case system the conceptual work process description for the autonomous transportation was created. It defines the operation of the autonomous transportation from the loading point to the unloading point and back, roles of the operators (machine drivers in the loading and unloading points) and the supervisor. Following the work process description, the hierarchical control structure for STPA was modelled and the control actions, feedback information and other related information was defined between the human controllers and the technical system elements. A simplified model of the control structure in this case is illustrated in Figure 4. Control actions can in this case be voice commands and instructions via radio, actions of the drivers via control devices and user interfaces, and system internal control signals and messages via data bus or cables.

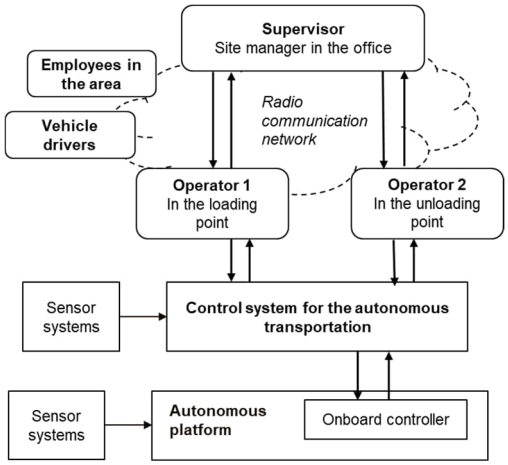

Figure 4. Outline of the control structure of the autonomous transportation system

To find possible unsafe control actions (UCAs) that could lead to a hazard in the operation of the autonomous vehicle the control structure was systematically analysed in the defined operational context and all foreseen worst-case situations. STPA method guides the analysis for UCAs by defining four different types of deviations in which a control action might become unsafe [4]. The main output from STPA are the loss scenarios describing causal relationships between the contributing factors in UCAs giving rise to a loss. Some examples of the loss scenarios related to autonomous driving during mixed traffic operation are shown below.

- Supervisor defines a route that is blocked by an object or unsafe to drive. Supervisor has not up-to-date information about the site conditions or other ongoing operations.
- Operator 1 in the loading point does not see that there is an employee near the saw log cage and calls the autonomous vehicle to move under the cage. The vehicle moves forward while employee is near the moving vehicle and can be injured.
- Operator 2 in the unloading point provides route-change command to the autonomous vehicle at the intersection of the route. The drivers in other vehicles nearby are surprised by the unexpected movement and this can cause an unsafe traffic situation at the route.
- The control system does not provide stop command to the autonomous vehicle or does it too late when safety system has detected a person in front. Autonomous vehicle can overrun or crush a person.
- The onboard control system starts the vehicle unexpectedly when there is a person or other object in front.
- The onboard control system provides a steering command to wrong direction when it is driving in its route. The vehicle can collide with other vehicles or structures.

In this study STPA was continued by using a risk-based prioritization of the loss scenarios and by formulating system safety requirements from the loss scenarios. Three level risk-based ranking was done according to the estimated severity of the worst-case consequences.

- High priority = Loss of life or permanent injury
- Medium priority = Serious injury to people or significant damage to the autonomous vehicle or other vehicles or the autonomous transportation is stopped for a long time
- Low priority = slight damage to the autonomous vehicle or other vehicles or delays in the autonomous transportation or problems in other daily operations at the site.

4 DISCUSSIONS

In this study PHA was used for identifying hazards and hazardous situation caused by the autonomously moving vehicle, actions of the system operators or actions of vehicle drivers and workers at the site. Also, possible system failures in technical systems were considered. In PHA the analysis scope was the overall system concept, its operation, and operating environment and possible traffic situations in the route of the autonomous vehicle. STPA was used to model the system controls by using the hierarchical control model for identification of actions that in certain circumstances can turn to unsafe control actions and cause hazardous situations or problems for the logistic process. The types of control actions that were analysed were different in different hierarchy level of the complex socio-technical system. They were human communications and instructions via radio, control commands given via user interfaces, or programmatic messages or wired signals between the control system elements and the autonomous vehicle. STPA focused on the control of the overall system and interactions between system controllers – both human operators and technical controllers. The concrete outcome of the combined analyses and risk assessments in terms of the case system concept were information of hazards and risks and proposals for risk reduction options and requirements for safety measures to be considered when developing safe autonomous transportation for saw logs.

The approach utilizing PHA and OHA methods in early system lifecycle phases has been successfully applied in several automated work-machinery applications in mining and cargo handling sectors [6][2]. The results of this study on autonomous saw log transportation concept and our practical experience using the PHA and STPA methods confirm the results of our earlier studies that in conceptual design phase STPA complements the PHA and adds value to the preliminary system safety analysis and risk assessment process. PHA reveals hazards that can directly affect personal safety, e.g., mechanical hazards, fire hazards, human errors. As a result, PHA gives information e.g., about the necessary safety distance to minimize the risk of collision. STPA reveals situations where control action can cause hazardous consequences due to e.g., insufficient command chains, wrong timing, missing information, or external impacts. which PHA cannot. The results are also in line with the results on other domains. Leveson (2018) have stated that STPA can be used in several different phases of a system engineering

process, starting in the earliest concept development stage as experienced in this study [7]. STPA can be used to generate high-level safety requirements early in the concept development phase, refine them in the system requirements development phase. The system requirements and constraints can then assist in the design of the mixed traffic operation, system architecture and more detailed system design and development. The results are also in line with the approach presented in safety engineering standards ISO 17757:2019 [8] and ANSI/UL 4600:2020 [9] that recommend to use different types of safety analysis methods at the beginning of the life cycle of autonomous systems to provide sufficient coverage of the socio-technical aspects of the mixed-fleet operation concept and to highlight different perspectives on the operation and operation of the complex system. ISO 17757:2019 describes the risk assessment process for autonomous or semi-autonomous machine systems [8]. ANSI/UL 4600:2020 defines requirements for autonomous vehicle systems and strongly recommends to use of different analysis methods for identification of autonomy related hazards and assessing risks [9].

Based on the results it can be concluded that PHA and STPA both aim to identify and define system-level characteristics, operating conditions or system behaviour that are needed to prevent system hazards and losses or control risks. The output of the concept level assessment of risks related to autonomy aspects forms the basis for system safety goals for the next life cycle phases and more detailed safety engineering activities. STPA complements the perspectives of traditional PHA and provides a formal presentation to connect losses - system level hazards - risk control options. However, it is strongly highlighted in studies on safety of autonomous work machine applications that the so-called predetermined risk analysis and risk assessment approach represented e.g., by PHA and STPA is not enough. Autonomous machine systems that can make safety critical control decisions need dynamic risk assessment capability to ensure safe operation in changing operating conditions and environments [10]. The autonomous machine systems especially in mixed traffic applications should be able to judge each situation independently and choose a suitable action based on internal dynamic risk assessments. This places a great emphasis on the situational awareness abilities of the system because they are needed to sense and determine the safety of the current and future states of the machine [11].

ACKNOWLEDGEMENT

This study is part of the research project ‘Artificial Intelligence using Quantum measured Information for real-time distributed systems at the edge’ (A-IQ Ready). The project is mainly funded by EU and Business Finland.

REFERENCES

1. INCOSE. 2015. Systems Engineering Handbook: A Guide for System Life Cycle Processes and Activities. John Wiley and Sons, Inc., USA. ISBN: 978-1-118-99940-0.
2. Tiusanen, R., Heikkilä, E. & Malm, T., 2021, System Safety Engineering Approach for Autonomous Mobile Machinery. 14th WCEAM Proceedings. Crespo Márquez, A., Komljenovic, D. & Amadi-Echendu, J. (eds.). Springer, p. 239-251 13 p. (Lecture Notes in Mechanical Engineering).
3. Rausand, M. 2005 Preliminary Hazard Analysis. System Reliability Theory (Second ed), Wiley. https://kntu.ac.ir/DorsaPax/userfiles/file/Mechanical/OstadFile/kazerooni2/PreliminaryHazardAnalysis.pdf
4. Leveson, N. & Thomas, J., 2018, STPA Handbook. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
5. SAE J3187:2022, System Theoretic Process Analysis (STPA) Recommended Practices for Evaluations of Automotive Related Safety-Critical Systems.
6. Tiusanen, R., An approach for the assessment of safety risks in automated mobile work machine systems. Dissertation. Espoo: VTT. 2014. https://publications.vtt.fi/pdf/science/2014/S69.pdf
7. Leveson, N. Safety Analysis in Early Concept Development and Requirements Generation. 28th Annual INCOSE International Symposium. July 7-12. 2018. Washington, DC, USA.
8. ISO 17757:2019 Earth-moving machinery and mining -- Autonomous and semi-autonomous machine system safety
9. ANSI/UL 4600:2020 Standard for Evaluation of Autonomous Products. UL Standards.
10. Heath, T., 2018, Autonomous Industrial Machines, and the Effect of Autonomy on Machine Safety. Tampere University of Technology. Master of Science Thesis, 62 pages.
11. Wardziński, A., 2008, Safety Assurance Strategies for Autonomous Vehicles. Computer Safety, Reliability, and Security, Springer, Berlin, Heidelberg, pp. 277-290.